

1  
2                   **APPLICATION**  
3                    *for*  
4                   **UNITED STATES LETTERS PATENT**  
5                   *by*  
6

7                   **NICHOLAS N. NASSIRI**  
8  
9

10                  *on the invention entitled*  
11  
12

13                  **SYSTEM AND METHOD OF IDENTITY AND SIGNATURE AND**  
14                  **DOCUMENT AUTHENTICATION USING A VIDEO CONFERENCE**  
15  
16

17                  **Pages of Specification: 72**  
18                  **Pages of Drawing: 3**  
19

20                  TO ALL WHOM IT MAY CONCERN:  
21

22                  BE IT KNOWN THAT I, Nicholas Nassiri, a citizen of the USA,  
23 has invented a new and useful method and system of performing  
24 identity and signature and document authentication using a  
25 videoconference of which the following is a specification:  
26  
27

1           **SYSTEM AND METHOD OF IDENTITY AND SIGNATURE AND**  
2           **DOCUMENT AUTHENTICATION USING A VIDEO CONFERENCE**

5           **Copyright Notice**

6           A portion of the disclosure of this patent document  
7           contains material that is subject to copyright protection.  
8           The copyright owner has no objection to the facsimile  
9           reproduction by anyone of the patent document or patent  
10          disclosure as it appears in the Patent and Trademark  
11          Office, patent file or records, but otherwise reserves all  
12          copyright rights whatsoever.

16          **BACKGROUND OF THE INVENTION**

18          **Field of the Invention**

19          The present invention relates generally to video  
20          conferencing and video communications and applications  
21          based on the technology thereof and more specifically it  
22          relates to an electronic method of identity and signature  
23          and document authentication via a "real time" live video  
24          conference exchange.

25          ///  
26          ///  
27          ///

1   **DESCRIPTION OF THE PRIOR ART**

2   It can be appreciated that methods of video conferencing  
3   have been in use for years. Typically, there exists a range  
4   of video conference systems or video communication systems  
5   that utilize a variety of structures, such as telephone,  
6   personal computers and mounted cameras to relay live stream  
7   video, and a variety of methods to facilitate the live  
8   stream conference. The prior art discloses United States  
9   Letters of Patent 5,991,276 issued to Yamamoto; United  
10   States Letters of Patent 6,124,882 issued to Voois et al;  
11   United States Letters of Patent 6,121,998 issued to Voois  
12   et al; United States Letters of Patent 6,128,033 issued to  
13   Friedel et al; and United States Letters of Patent  
14   6,037,970 issued to Kondo.

15   The Yamamoto patent depicts a multipoint videoconference  
16   system which delivers video and voice information along  
17   with various types of material data to realize a more  
18   realistic teleconferencing environment. The system  
19   comprises a plurality of videoconference terminals, a  
20   videoconference server, and a videoconference  
21   administration server. The videoconference administration  
22   server controls network connections between the  
23   videoconference server and the videoconference terminals.  
24   The Yamamoto patent does not depict a method and system of  
25   identity and signature and document authentication via a  
26   "real time" live stream video conference format.

27   The Vois patent number 6124882 depicts a videophone device  
28   that utilizes a programmable processor circuit

1 capable of communicating over a conventional communications  
2 channel, such as a POTS line, and of generating video data  
3 for display on a television set. The device includes a  
4 video source, an interface circuit, including a modem  
5 transmitting and receiving video and audio data over the  
6 channel; a circuit for storing a program to control the  
7 videophone apparatus; and a display driver circuit for  
8 generating video data to the display. The Vois patent  
9 number 6124882 does not depict a method and system of  
10 identity and signature and document authentication via a  
"real time" live stream video conference format.

11  
12 The Vois patent number 6121998 depicts a programmable  
13 video/general-purpose processor capable of readily updating  
14 program-related data. The processor includes a first  
15 circuit section used to process data for videoconferencing  
16 and to detect codes data used for revising software-related  
17 data provided from a remote location, and a second circuit  
18 section used for executing the executable program data  
19 stored in the second memory circuit. A volatile memory  
20 circuit is coupled to and accessed by the programmable  
21 video/general-purpose processor, and is used for storing  
22 the revision data until it is validated. The non-volatile  
23 memory circuit is then used by the processor in a  
24 subsequent video-related application, such as a  
25 videoconferencing application or a web browser application.  
26 The Vois patent does not depict a method and system of  
27 identity and signature and document authentication via a  
"real time" live stream video conference format.

1       The Friedel patent depicts an audiovisual communications  
2       terminal apparatus that is adapted for interconnection to  
3       at least one other audiovisual communications terminal  
4       apparatus by a communications medium to form an audiovisual  
5       teleconferencing network. The audiovisual communications  
6       terminal apparatus includes an interface device, producing  
7       and transmitting means, and receiving and broadcasting  
8       means. The interface device operates to condition input  
9       audiovisual signals received from the other audiovisual  
10      communications terminal apparatus and to condition output  
11      audiovisual signals for processing by the other audiovisual  
12      communication terminal apparatus. The receiving and  
13      broadcasting means receive the input audiovisual signals  
14      from the interface device and broadcast the received input  
15      audiovisual signals thereby creating an audiovisual  
16      teleconference between two users so that the users can both  
17      see and hear each other. The Friedel patent does not  
18      depict a method and system of identity and signature and  
19      document authentication via a "real time" video conference  
20      format.

21      The Kondo patent depicts a videoconference system that  
22      conducts a videoconference among a plurality of  
23      communication centers which are connected by a  
24      communication line. Each communication center includes:  
25      display devices for displaying images from the other  
26      communication centers participating in the videoconference;  
27      speaker devices for outputting voices from the other  
28      communication centers participating in the videoconference;  
          camera devices disposed at positions corresponding to the

1 display devices, for imaging participants in the  
2 videoconference; microphone devices disposed at positions  
3 corresponding to the display devices, for capturing voices  
4 from the participants; and a transmitter/receiver  
5 transmitting output signals from the camera devices and  
6 output signals from the microphone devices to the other  
7 communication centers, and receiving output signals from  
8 the camera devices and output signals from the microphone  
9 devices of the other communication centers, the  
10 transmitter/receiver for supplying the output signals from  
11 the camera devices and the output signals from the  
12 microphone devices of the other communication centers to  
13 the display devices and the speaker devices corresponding  
14 to the camera devices and the microphone devices. The Kondo  
15 patent does not depict a method and system of identity and  
16 signature and document authentication via a "real time"  
17 live stream video conference format.

18 The above methods have been widely used in the commercial  
19 marketplace in various business practices. For example,  
20 found in the marketplace are businesses that utilize live  
21 stream video conferencing to facilitate certain  
22 communication-based transactions between parties that are  
23 geographically remote. The research discloses practices  
24 that utilize video conferencing to facilitate transactions  
25 such as "remote arraignment" whereby live stream video  
26 connects judicial agencies (courts) to penal institutions  
27 (where the prisoner resides), thereby enabling the parties  
28 to conduct criminal arraignments from remote locations.

Likewise, the research discloses practices that utilize video conferencing to facilitate transactions such as "remote education" whereby educational facilities (the physical classroom) broadcast their lectures to remote locations (one's television set or desktop computer) via live stream video.

The prior art and prevailing business practices clearly illustrate the usefulness and many benefits of systems and methods of videoconference. Great amounts of time and money are saved by uniting geographically remote individuals. Businesses, governmental agencies, consumers, students, and the like benefit from being able to bridge the distance between geographically remote parties. While the prior art discloses very useful means and benefits, existing methods, while joining the remote parties during the live videoconference, fail to facilitate particular transactions during the videoconference: signature authentication, identity authentication or document creation and authentication.

The method of the present invention functions to facilitate any of the foregoing requests singularly, or all of the requests simultaneously. That is: the present invention may capture a signature, a photograph, biometric data or other forms of electronic data and create an authenticated electronic document using said data input. To put into context: parties that are not familiar with one another may have a need to authenticate the identity of the remote party with whom they videoconference with. For example, two

1 geographically dispersed parties wish to execute a single  
2 document to conclude a transaction: such as the sale and  
3 subsequent purchase of property. The commercial transaction  
4 of the transfer of the real estate property is dependent on  
5 verifying the identity of a party to the videoconference,  
6 and obtaining the respective signatures of the parties.  
7 Methods of signature/identity authentication may include,  
8 but are not limited to, electronic signature capture,  
9 biometric data capture, photograph capture, or electronic  
10 data capture during a live videoconference exchange. The  
11 commercial real estate transaction involves the  
12 geographically remote parties each individually,  
13 nonetheless simultaneously, signing a single electronic  
14 document necessary to conclude the transaction, such as a  
15 promissory note. Upon the respective electronic data input  
16 from the geographically remote parties, such respective  
17 electronic data input from each party is verified, and  
18 fused in a single, authenticated electronic document.

19 The prior art fails to disclose any videoconference method  
20 whereby signature authentication or identity authentication  
21 may be conducted during the videoconference. The prior art  
22 fails to disclose any videoconference method whereby  
23 electronic data may be captured and input during the video  
24 conference. The prior art fails to disclose any  
25 videoconference method whereby the respective electronic  
26 data input from any party is verified, and fused in a  
27 single, authenticated electronic document.

28 The main problem with conventional real time video

1 conferencing methods is that none of the existing systems  
2 or applications incorporate a system, method or process of  
3 electronic identity authentication of the geographically  
4 remote individuals to the videoconference.

5 Another main problem with conventional real time video  
6 conferencing methods is that none of the existing systems  
7 or applications incorporate a system, method or process of  
8 electronic signature authentication of the geographically  
9 remote individuals to the videoconference.

10 Another problem with conventional real time video  
11 conferencing methods is that none of the existing systems  
12 or applications incorporate a system, method or process of  
13 electronic document authentication as part of the  
14 transaction by the geographically remote individuals to the  
15 videoconference.

16 Another problem with conventional real time video  
17 conferencing methods is that none of the existing systems  
18 or applications incorporate a system, method or process of  
19 electronic authentication of one's identity, signature and  
20 the documents simultaneously of the geographically remote  
21 individuals to the videoconference.

22 Another problem with conventional real time video  
23 conferencing methods is that none of the existing systems  
24 or applications incorporate a system, method or process of  
25 electronic authentication of one's identity, signature or  
26 documents utilizing biometric data that is conveyed during  
27 the video conference.

1       While the prior art devices and methods may be suitable for  
2       the particular purpose to which they address, they are not  
3       suitable for real time, live stream electronic  
4       authentication of an identity, a signature, or real time  
5       live stream electronic document creation and  
6       authentication; whether the said identity, signature, or  
7       electronic document is authenticated individually or in  
conjunction with at least one other verification request.  
8

9       In these respects, the method of electronic identity and  
10      signature and document authentication via a real time, live  
11      stream videoconference exchange, according to the present  
12      invention, substantially departs from the conventional  
13      concepts and designs of the prior art, and in so doing  
14      provides an apparatus primarily developed for the purpose  
15      of an electronic method of identity and signature and  
16      document creation and authentication via a real time, live  
video conference exchange.

1      **SUMMARY OF THE INVENTION**

2  
3      The general purpose of the present invention, which will be  
4      described subsequently in greater detail, is to provide a  
5      new method of real time video conference for electronic  
6      identity and signature authentication, and for electronic  
7      document creation and authentication, that has the many  
8      advantages mentioned heretofore and many novel features  
9      that result in a new videoconference method which is not  
10     anticipated, rendered obvious, suggested, or even implied  
11     by any of the prior art video conferencing, either alone or  
in any combination thereof.

12  
13     The present invention incorporates a variety of  
14     applications and technology that in conjunction can be used  
15     to authenticate a personal identity, a signature, or an  
16     electronic document, either singularly or simultaneously,  
17     during a real time, live stream videoconference. The nature  
18     of the transaction is dependent on the needs of the parties  
19     to the videoconference. For example, the parties may need  
20     identity authentication, or signature authentication, or  
21     electronic document creation and authentication, or a  
combination of all three.

22  
23     Likewise, the form and type of authentication will vary  
24     depending on the needs or requests of the parties. The  
25     present invention is capable of a broad base of  
26     applications that result in authentication. The method of  
27     the present invention utilizes signature data, biometric  
28     data, photographs, electronic data input and electronic

1 notarization. Any particular form of authentication may be  
2 used singularly or in conjunction with another form of  
3 authentication. The purpose of the electronic data capture  
4 is to create an authenticated document, such as an executed  
5 contract, a passport or drivers license, and the like. The  
6 present invention is capable of authenticating any type of  
7 document and the foregoing examples are not regarded as  
8 limiting. Likewise, it should be understood that the  
9 foregoing examples of authentication are all conducted  
10 between geographically remote parties during a real time,  
11 live stream videoconference.

12 By way of example, a standard real estate transaction is  
13 detailed. Such a transaction typically requires that  
14 geographically remote parties physically meet to confirm  
15 the identity of one another or that they travel to a notary  
16 public to have their identities authenticated. Such a  
17 process is time consuming, expensive and inconvenient.  
18 Using the present invention, a transfer of title to  
19 property would unite the buyer in New Jersey, the seller in  
20 California, and the e the notary public in New York in a  
21 three way real time, live stream video conference. The  
22 geographically remote parties are each able to view one  
23 another via a video and audio stream. The parties may each  
24 input electronic data, in this instance, a signature, into  
25 a single electronic document using the means of the present  
26 invention. Upon input of the respective electronic data  
27 from the dispersed parties, the present invention serves to  
28 manage the electronic data input and generate the desired

1 electronic document. By way of the foregoing example, the  
2 result would be a single, authenticated electronic document  
3 that is executed by the dispersed parties. A time and date  
4 stamp is affixed to the electronic document so that no  
5 changes may be made to the encrypted document. The single,  
6 finalized notarized electronic document is then issued to  
7 the authorized receiving party, such as the registrars  
8 office.

9 In another embodiment, the present inventive method enjoins  
10 a customer with a remote governmental agency in a real  
11 time, live stream videoconference. In this embodiment, the  
12 present invention inputs electronic data from the customer  
13 for the purpose of creating an authenticated government  
14 issued document, such as a drivers license or a passport.  
15 Per the foregoing example, the electronic data input may  
16 comprise various forms, including, but not limited to, an  
17 electronic signature, a photographic image, biometric data,  
18 such as a thumbprint, or electronic data in the form of a  
19 code or a password. Using the inventive device, said  
20 governmental agency in turn verifies the electronic data  
21 input as being authentic. Upon authentication of the input  
22 information, an electronic document is created that  
23 encapsulates the input electronic data with the document  
24 requested, such as a passport or social security card.

25 In another embodiment of the present invention, a customer  
26 accesses the present invention by way of the world wide web  
27 (WWW). In this embodiment, the customer initiates a real  
28 time, live stream videoconference with a remote site from a

1 location of the customer's choice, such as the home or the  
2 office. Per the foregoing methods, the customer will be  
3 prompted to input varied forms of electronic data,  
4 including, but not limited to, an electronic signature, a  
5 photographic image, biometric data, such as a thumbprint,  
6 or electronic data in the form of a code or a password. The  
7 remote site verifies the input data and in turn creates an  
8 authenticated document that is issued to the authorized  
9 party, such as a government agency, a medical practitioner,  
a lawyer, and the like.

10  
11 The WWW embodiment is put into context by way of the  
12 following example. Assume that a customer requires an  
13 authenticated student identification card. The customer  
14 need not travel to the university for the creation of such  
15 a card but may input the required information from the  
16 convenience of home. The customer accesses the present  
17 invention on the WWW using a configured graphic user  
18 interface (GUI). Utilizing the GUI, the customer may input  
19 electronic data using a home personal computer. The  
20 customer will be prompted to input varied forms of  
21 electronic data, including, but not limited to, an  
22 electronic signature, including a graphical hand written  
23 signature, a photographic image, biometric data, such as a  
24 thumbprint, or electronic data in the form of a code or a  
25 password. The electronic data input is verified by the  
26 present inventive method and amalgamated into an  
authenticated student card which is issued to the  
authorized party, presumably the student in this instance.

27  
28 In any of the embodiments of the present invention,

Confidential

Page 14

9/28/2001

1           irrespective of the type of service request, whether it be  
2           an executed, notarized electronic document or an  
3           authenticated identification card, electronic data input by  
4           the parties participating in the videoconference may be  
5           input singularly or simultaneously. Likewise, input data  
6           may comprise various forms of electronic data in a single  
7           session, such as: an electronic document, a digital  
8           certificate, an electronic notary seal, biometric data, a  
9           password or a code, a photographic image and other such  
10          data input. Any data input from any party to the  
11          videoconference is transmitted via a real time, live stream  
12          during the course of the videoconference. Any data input  
13          from any party to the videoconference that is transmitted  
14          during the course of the videoconference, may be  
15          transmitted either singularly or simultaneously by the  
16          parties. The input data is subsequently fused to an  
17          electronic document and issued to the authorized party.

18         The above referenced examples illustrate that the present  
19         invention is comprised of various technologies that work in  
20         conjunction with one another or individually to comprise  
21         the method of electronically authenticating one's identity,  
22         a signature or a document in real time, live stream video  
23         format. To these ends, the present invention is comprised  
24         of the following components:

- 25           (i)      a multi-point and multi-media video conference system  
26                    (including fixed and portable structures);  
27           (ii)     an electronic signature capture device;

- (iii) the means to authenticate the electronic signature input by way of the electronic signature capture device;
  - (iv) a device to create electronic documents;
  - (v) the means to authenticate electronic documents;
  - (vi) an electronic document repository;
  - (vii) a device to create a digital certificate;
  - (viii) the means to authenticate a digital certificate;
  - (ix) a device to create an electronic time and date stamp;
  - (x) the means to authenticate an electronic time and date stamp;
  - (xi) a device to create an electronic notary seal (detailed in USPTO patent-pending application, identified as Customer 021907);
  - (xii) the means to authenticate an electronic notary seal (detailed in USPTO patent-pending application, identified as Customer 021907);
  - (xiii) a device or devices to capture biometric data, such as a fingerprint, photographic image and the like;
  - (xiv) the means to authenticate biometric data, such as a fingerprint, photographic image and the like;
  - (xv) a device to fuse the electronic data input with an electronic document;
  - (xvi) the means to authenticate an electronic document that has electronic data fused to it; and
  - (xvii) such other applications and or devices which are necessary to facilitate the function of the aforementioned components whether individually or in conjunction with one another.

1       The primary object of the present invention is to provide  
2       an electronic method of personal identity, signature, and  
3       electronic document authentication using a real time, live  
4       stream videoconference platform that overcomes the  
5       shortcomings of the prior art devices.  
6

7       Another object of the present invention is to provide a  
8       method of identity, signature, and electronic document  
9       authentication using a real time, live stream  
10      videoconference platform that will facilitate electronic  
11      commerce: particularly transactions that involve sensitive  
12      data or high value transactions.

13      Another object of the present invention is to provide a  
14      method of identity, signature, and electronic document  
15      authentication using a real time, live stream  
16      videoconference platform that integrates real time  
17      electronic data input to facilitate electronic commerce  
18      transactions wherein such transactions require the input of  
19      personal data, such as an electronic signature or scanned  
20      fingerprint.

21      Another object of the present invention is to provide a  
22      method of identity, signature, and electronic document  
23      authentication using a real time, live stream  
24      videoconference platform that can electronically notarize  
25      electronic documents.

26      Another object of the present invention is to provide a  
27      method of identity, signature, and electronic document

1 authentication using a real time, live stream  
2 videoconference platform that authenticates the identity of  
3 a party to a transaction via a variety of methods,  
4 including, but not limited to, electronically transmitted  
5 biometric data, personal identification papers, in digital  
6 and hard-copy format, codes, encryption keys, passwords or  
7 other preordained formulas.

8 Another object of the present invention is to provide a  
9 method of identity, signature, and electronic document  
10 authentication using a real time, live stream  
11 videoconference platform that allows a plurality of  
12 individuals to each individually, but simultaneously,  
13 witness the respective individual input electronic data  
14 into an electronic document, such as an electronic  
15 signature or an electronic fingerprint.

16 Another object of the present invention is to provide a  
17 method of identity, signature, and electronic document  
18 authentication that will allow an individual, via an  
19 interface with the present invention, direct communication  
20 with government agencies that require authentication of  
21 either the individual's identity, signature, or documents  
22 prior to issuing a government issued document or benefits.

23 Another object of the present invention is to provide a  
24 method of identity, signature, and electronic document  
25 authentication using a real time, live stream  
26 videoconference platform that fuses the electronic data  
27 input by the parties to the electronic documents created

1 through the method of the present invention.

2  
3 Another object of the present invention is to provide a  
4 method of identity, signature, and electronic document  
5 authentication using a real time, live stream  
6 videoconference platform that allows an individual, via an  
7 interface with the present invention, direct communication  
8 with government and other regulatory agencies to create  
9 hard copy identity-based cards or documents that are  
encoded with various electronic and biometric information.

10  
11 There has thus been outlined, rather broadly, the more  
12 important features and objectives of the invention in order  
13 that the detailed description thereof may be better  
understood, and in order that the present contribution to  
the art may be better appreciated. There are additional  
14 features of the invention that will be described  
15 hereinafter.

16  
17 Other objects and advantages of the present invention will  
18 become obvious to the reader and it is intended that these  
19 objects and advantages are within the scope of the present  
20 invention. In this respect, before explaining at least one  
21 embodiment of the invention in detail, it is to be  
22 understood that the invention is not limited in its  
23 application to the details of construction and to the  
24 arrangements of the components set forth in the following  
25 description or illustrated in the drawings. The invention  
26 is capable of other embodiments and of being practiced and  
27 carried out in various ways. Also, it is to be understood

1           that the phraseology and terminology employed herein are  
2           for the purpose of the description and should not be  
3           regarded as limiting.

4           To the accomplishment of the above and related objects,  
5           this invention may be embodied in the form illustrated in  
6           the accompanying drawings, attention being called to the  
7           fact, however, that the drawings are illustrative only, and  
8           that changes may be made in the specific construction  
9           illustrated.

1   **BRIEF DESCRIPTION OF THE DRAWINGS**

2  
3   Various other objects, features and attendant advantages of  
4   the present invention will become fully appreciated as the  
5   same becomes better understood when considered in  
6   conjunction with the accompanying drawings, in which like  
7   reference characters designate the same or similar parts  
8   throughout the several views, and wherein:

9                 FIG.1         Figure 1 depicts the general routing process  
10          of a request for identity or signature authentication. The  
11          distinction between the "public" and "private" domain is  
12          whether the request involves a government/ regulatory  
13          entity. The former designation being deemed a "public"  
14          process whereby the signature or identity authentication is  
15          for the purpose of authenticating a government or a  
16          regulatory based identity document. The latter designation  
17          being deemed a "private" process whereby the signature or  
18          identity authentication is for the purpose of a commercial  
19          transaction.

20                 FIG. 2         Figure 2 depicts the steps and/or methods  
21          utilized to authenticate an identity or signature.

22                 FIG.3         The present invention processes' are somewhat co-  
23          dependent insofar that the process of either identity and  
24          signature verification inherently result in an  
25          authenticated document. Figure 3 depicts the steps and/or  
26          methods utilized to create, secure and store an electronic  
27          document.

1       The drawings are intended to provide an over-view of the  
2 processes of the present invention. There exist various  
3 technological applications by which the objectives of the  
4 present invention can be realized. The various means or  
5 methods by which authentication shall be established are  
6 specifically set forth in the embodiment of the invention  
7 as put forth below.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1   **DESCRIPTION OF THE PREFERRED EMBODIMENT**

2  
3   The present invention recognizes that there is much more to  
4   live stream videoconference collaboration than just the  
5   video and audio experience. The present invention offers  
6   solutions that blend video and audio communication with  
7   various forms of electronic data input with a real time,  
8   live stream videoconference. Specifically, the present  
9   invention is a process, method and system that uses a  
10   videoconference system to input and transmit electronic  
11   data for the purpose of authenticating an identity, a  
12   signature or to create an authenticated electronic document  
13   using a real-time, live-stream videoconference medium.

14  
15   The present invention is useful and efficient because the  
16   inventive device is open-ended in application. The present  
17   invention can be applied, but is not limited to, the  
18   following transactions: any transaction that requires  
19   authentication of an identity; any transaction that  
20   requires authentication of a signature; or any transaction  
21   that requires authentication of an electronic document. The  
22   method of the present invention is best suited where the  
23   parties to the transaction are geographically remote, and  
24   can be utilized for any e-commerce based transaction that  
25   requires authentication of either an identity, a signature,  
26   or a document; or any transaction where the parties require  
27   authentication of either an identity, a signature to issue  
28   an identity-based document, such as a passport or a drivers  
   license. The creation and authentication of electronic  
   documents or identity-based documents occurs during the

1 course of the real time, live stream video conference using  
2 electronic data input by geographically remote parties to  
3 the transaction.

4  
5 The present invention is premised on the concept of an  
6 increasingly borderless world, insofar as technology and  
7 the Internet have ever more united remote parties in a host  
8 of transactions that once would have necessitated an  
9 actual, physical face-to-face meeting. By way of example,  
10 one may execute electronic documents online on the Internet  
11 using forms of electronic signatures, thereby eliminating  
12 the need for the signatories to coordinate a face-to-face  
13 meeting. Likewise, one may scan personal biometric data,  
14 such as a thumbprint, and submit such data via an  
15 electronic upload to a remote database, thereby eliminating  
16 the need to manually fingerprint oneself and mail such hard  
17 copy information. Remarkably, with ease we now  
18 videoconference using desktop computers and telephonic  
19 devices that allow geographically remote parties to  
simultaneously view and hear one another via the Internet.

20 All of these technologies function to eliminate the need to  
21 arrange an actual physical meeting to facilitate a host of  
22 transactions. The present invention seeks to coordinate  
23 such borderless processes for a method and system of remote  
24 party collaboration not rendered by the prior art using a  
25 real time, live stream videoconference to enjoin the  
26 parties. In the preferred embodiment of the present  
27 invention, a customer accesses a remote facility to  
process a verification request of the customer's

1 identity or the customer's signature, with the purpose of  
2 the verification to create an authenticated electronic  
3 document.

4  
5 The remote facility is a physical location with the  
6 physical infrastructure and means necessary for the present  
7 invention to function, referred to herein as the "Video  
8 Verification Service Center" (VVSC). The VVSC is a place of  
9 business that allows geographically remote parties to  
10 conduct transactions by way of a videoconference that  
11 functions to transmit varied electronic data from  
12 participants to the videoconference, such as an electronic  
13 signature, a photographic image, a fingerprint, or other  
such electronic data in the course of a videoconference.

14  
15 Secondly, the VVSC functions to create electronic documents  
16 using the input electronic data, such as a graphical, hand  
17 written signature, an electronic signature using a digital  
18 certificate, a fingerprint or a photograph during the  
19 course of a videoconference. The end result being that the  
20 participant's biometric information and personal  
21 information are fused to an authenticated document. An  
22 authenticated document may comprise an executed deed of  
23 trust whereby the parties electronic signatures are affixed  
24 to the electronic document as a means of authentication, or  
25 a drivers license or a passport, whereby the parties  
26 electronic signatures and other information such as a  
thumbprint and photographic image are affixed to the  
electronic document as a means of authentication.

27       ///

28       ///

1           **APPLICATIONS OF THE PRESENT INVENTION**

2           **I. Identity, Signature, and Document Authentication Using a**  
3           **VVSC**

4  
5           To put the system and method of the present invention into  
6           context of a specific transaction: two parties that are  
7           geographically remote must each individually sign a single  
8           document and have each of their respective signatures  
9           notarized by a notary public. Each party goes to an  
10          independent VVSC that is conveniently located in proximity  
11          with their physical location. The VVSC initiates a  
12          videoconference with all of the parties to the transaction,  
13          including a notary public. The videoconference comprises  
14          screens or monitors at each location whereby the parties  
15          can input and receive audio, visual and electronic data  
16          simultaneously, albeit independently at each location.

17          Upon initiation of the videoconference, VVSC downloads the  
18          electronic document to a central host computer that is to  
19          be signed by the parties and that is to be notarized  
20          by the notary public. The electronic document to be  
21          downloaded may be provided in a portable format, such as a  
22          diskette or compact disc and is provided by one of the  
23          parties to the transaction. Alternatively, the electronic  
24          document may be downloaded from a repository of electronic  
25          documents maintained by the present invention.

26          Each VVSC has access to the single host computer where the  
27          electronic document has been downloaded. The downloaded  
28          electronic document is displayed on a screen or monitor

1 for the respective parties to see, each party viewing the  
2 same electronic document. Likewise, the screen or monitor  
3 comprises split images that are viewed simultaneously: one  
4 of the remote party, one of the electronic document to be  
5 signed, one of the electronic data being input and other  
6 such multiple imaging as necessary.

7 Each party executes the electronic document by inputting an  
8 electronic signature that is affixed to the electronic  
9 document. Electronic signature input may comprise several  
10 methods, including, but not limited to, a signature capture  
11 device, by biometrics, by a digital certificate, or by a  
12 password or code. In the preferred embodiment, each party  
13 affixes a graphical, hand written signature using a  
14 signature capture device. The present invention comprises  
15 the means to affix the graphical, hand written signature to  
16 the electronic document. In another embodiment, the  
17 electronic signature may be in the form of a digital  
18 certificate or other form of source code that is input by  
19 the parties to the transaction.

20 The present invention further comprises the means whereby  
21 as each party electronically signs the electronic document,  
22 the electronic data being input is displayed on the screen  
23 or the monitor. Each party to the videoconference is  
24 thereby viewing a single screen with dual images: the other  
25 parties, the electronic document, and the electronic  
26 signature as it is being captured. In the preferred  
27 embodiment the other party thus witnesses the other party  
28 signing the electronic document in one image,  
simultaneously sees the ensuing signature as a separate

1           dual image and the electronic document as a separate dual  
2           image.

3  
4           Upon affixation of each electronic signature to the single  
5           electronic document, the screen or monitor will depict the  
6           signed electronic document. In the preferred embodiment,  
7           the electronic data may be affixed to the electronic  
8           document as a visual representation. Alternatively, the  
9           electronic data may be affixed to the electronic document  
in the form of encrypted source code.

10  
11          Should other electronic data be required, such as a  
12          photographic image, a thumbprint, or a code, it will be  
13          entered in subsequent fashion and displayed on the screen  
or monitor. By way of example, in addition to affixing an  
14          electronic signature to the electronic document, the  
15          parties may request further authentication information such  
16          as a drivers license number, or a thumbprint. As such other  
17          authentication data is entered, the respective information  
18          is displayed on the screen or monitor as a separate image,  
19          and is affixed to the electronic document where indicated.  
20          In the preferred embodiment, the electronic data may be  
21          affixed to the electronic document as a visual  
representation. Alternatively, the electronic data may be  
22          affixed to the electronic document in the form of encrypted  
23          source code.

24  
25          Should notarization be required a notary public  
26          authenticates the document by verifying the identity of the  
27          signing parties and by affixing an electronic notary seal.

The notary public may be an employee who is physically located at the VVSC or may be a remote party enjoined by the videoconference. Electronic notarization parallels the customary legal form of notarization. The notary public shall require that the signatories provide such authentication information as required by law, typically a government issued photo identification card and a biometric submission, such as a signature or a thumbprint. VVSC employee notary public will have the means to verify hard copy personal identification, such as a drivers license information and to input said information electronically in the form of a source code. Likewise, VVSC employee notary public will have the means to verify the electronic signature of the party and to input said information electronically in the form of a source code. Per the methodology above, the input information is displayed on the screen or monitor as a separate dual image.

Upon input of the personal verification information, VVSC notary public affixes an electronic notary seal to the electronic document. In the preferred embodiment of the present invention, the electronic notary seal is in the form of a graphical representation of the notary public's seal. The graphical representation is affixed to the electronic document as a visual image. Alternatively, the notary seal may be affixed to the document in the form of a source code. Any changes to the electronic document will invalidate the notary public's seal.

Upon affixing all of the required authentication

1 information, including, but not limited to, an electronic  
2 signature, a photographic image, biometric information,  
3 source code, an electronic notary seal, a time and date  
4 stamp is applied and the electronic document is encrypted.

5 The signed, notarized electronic document is disseminated  
6 to the requesting party or parties. If the parties so  
7 desire, the VVSC shall archive a copy of the electronic  
8 document for future reference.

9  
10 In another embodiment of the invention, the parties to the  
11 transaction may request that a VVSC representative travel  
12 to a location of their choice, such as a home or an office.  
13 The VVSC representative is equipped with the necessary  
14 hardware and the means to facilitate transactions, as  
15 depicted above. The VVSC representative initiates a  
16 videoconference with the respective parties and with the  
17 VVSC itself. The above identified processes are adhered to.  
18 The traveling VVSC representative is useful in situations  
19 where the parties are unable to travel, such as the infirm  
20 or elderly, or in corporate environments that entail  
21 several parties to a transaction. Per the method of the  
22 preferred embodiment, the traveling VVSC representative may  
23 enjoin as many parties to the videoconference as necessary,  
24 including a notary public. Alternatively, the traveling  
25 VVSC representative may be a notary public.

26 As the foregoing example clearly illustrates, the present  
27 invention has the potential to facilitate transactions  
28 where the parties are in different cities, states or even

1 countries. The present invention is open-ended in  
2 application and could be used in any e-commerce transaction  
3 that requires some form of identity or signature  
4 authentication. An individual in New York may purchase a  
5 home in California or an automobile overseas. The present  
6 invention redresses a significant hurdle to conducting e-  
7 commerce, namely, the problem of identity fraud. VVSC  
8 authentication not only enables the parties to communicate  
9 via a real-time, live stream feed, it allows them to  
10 remotely conclude the transaction at hand by accessing a  
11 single electronic document simultaneously and inputting  
their respective personal information.

12

13 **II. Identity Card Creation Authentication Using a VVSC**

14 In another embodiment of the present invention, the  
15 inventive device functions to create personal-identity  
16 cards for regulatory agencies, educational institutions, or  
17 the private sector. This embodiment functions per the  
18 methodology of the first embodiment but with a different  
19 objective. As opposed to facilitating e-commerce  
20 transactions, the inventive device is used to verify  
21 identity and issue authoritative documents. By way of  
22 example, a government agency may require authoritative  
23 authentication to issue a state sponsored identification  
card, such as a passport, a social security number or a  
drivers license.

24

25 The customer requiring an identity-based document goes to  
26 an independent VVSC that is conveniently located in  
27 proximity with their physical location. The VVSC initiates

1       a videoconference with all of the parties to the  
2 transaction: the customer and the respective government  
3 agency. Per the preferred embodiment, the videoconference  
4 comprises screens or monitors at each location whereby the  
5 parties can input and receive audio, visual and electronic  
6 data simultaneously, albeit independently at each location.

7       Upon initiation of the videoconference, VVSC downloads the  
8 specific electronic document from the electronic document  
9 to a central host computer that is to become a particular  
10 identity-based document. The downloaded electronic document  
11 is displayed on a screen or monitor for the respective  
12 parties to see, each party viewing the same electronic  
13 document. Likewise, the screen or monitor comprises split  
14 images that are viewed simultaneously: one of the remote  
15 party, one of the identity-based electronic document to be  
16 created, one of the electronic data being input and other  
17 such multiple imaging as necessary.

18      The VVSC shall prompt the customer to provide such personal  
19 information as mandated by the requesting agency. Personal  
20 information may include, but is not limited to, biometric  
21 information, data entry of personal statistics, such as  
22 height, weight and birth date, an electronic signature and  
23 the like. The input of said personal information may  
24 comprise various forms, including, but not limited to,  
25 electronic signature input using a signature capture  
26 device, by biometrics, by a digital certificate, or by a  
27 password or code. In the preferred embodiment, the customer  
28 affixes a graphical, hand written signature using a

1           signature capture device to the identity-based electronic  
2           document.

3  
4           Per the method of the preferred embodiment, the present  
5           invention comprises the means whereby as the customer  
6           electronically signs the electronic document, the  
7           electronic data being input is displayed on the screen or  
8           the monitor of the requesting agency. The requesting agency  
9           to the videoconference is thereby viewing a single screen  
10          with dual images: the customer, the identity-based  
11          electronic document, and the electronic signature as it is  
12          being captured. Upon affixation of each electronic  
13          signature to the identity-based electronic document, the  
14          screen or monitor will depict the signed identity-based  
15          electronic document. In the preferred embodiment, the  
16          electronic data may be affixed to the electronic document  
17          as a visual representation. Alternatively, the electronic  
18          data may be affixed to the electronic document in the form  
19          of encrypted source code.

20         Should other electronic data be required, such as a  
21         photographic image, a thumbprint, or a code, it will be  
22         entered in subsequent fashion and displayed on the screen  
23         or monitor. By way of example, in addition to affixing an  
24         electronic signature to the electronic document, the  
25         requesting agency may request further authentication  
26         information such as a drivers license number, or a  
27         thumbprint. As such other authentication data is entered,  
28         the respective information is displayed on the screen or  
            monitor as a separate image, and is affixed to the

1           electronic document where indicated. In the preferred  
2 embodiment, the electronic data may be affixed to the  
3 electronic document as a visual representation.  
4 Alternatively, the electronic data may be affixed to the  
5 electronic document in the form of encrypted source code.

6           As the foregoing example clearly illustrates, the present  
7 invention has the potential to facilitate transactions  
8 where the parties are in different cities, states or even  
9 countries. An American traveler who loses a passport in  
10 India may find A VVSC, videoconference with the issuing  
11 authority, and have a new passport electronically created  
12 and issued without the wait, expense or inconvenience of  
13 traditional channels.

14           **III. Identity, Signature, and Document Authentication Using**  
15           **a Local Computer System and the World-Wide-Web**

17           In yet another embodiment of the present invention, the  
18 parties to the transaction utilize the inventive device  
19 independent of the VVSC and independent of a traveling VVSC  
20 representative. In this embodiment of the present  
21 invention, the parties to the transaction initiate a  
22 videoconference via a website that is a function of the  
23 VVSC. The web-based VVSC application has a two-fold  
24 function: it allows parties to conduct private transactions  
25 using a videoconference broadcast via the WWW  
26 (webconference), secondly, and it allows registered users  
27 to submit electronic data to the VVSC for retrieval and/or  
dissemination to other parties.

1 As a priori, to use the present invention from a location  
2 independent from a VVSC and independent of a traveling VVSC  
3 representative., i.e. the WWW, the customer first must  
4 register with the VVSC at its physical location.  
5 Registration comprises the VVSC obtaining and verifying  
6 personal information from the customer using a variety of  
7 data, such as electronic data, government issued personal  
8 identity documents, biometric data, such as an electronic  
9 signature, a thumbprint and the like, a digital certificate  
10 or other such data as may be available. Upon registration,  
11 VVSC issues the customer personal identification documents  
12 from VVSC, including, but not limited to, a digital  
13 certificate, a smart card, a password or a code. VVSC may  
14 keep a record of customer's biometric information for  
future use, should customer elect to do so.

15 To initiate a transaction independent of the VVSC, a  
16 customer wishing signature or identity verification or  
17 electronic document creation utilizes the present invention  
18 via a local computer system to interface with the VVSC  
19 website located on the World Wide Web (WWW). The customer  
20 accesses the website via the local computer system and logs  
21 in using the password or code as provided by VVSC in the  
22 registration process. As per the methodology depicted  
23 above, a videoconference is initiated by the VVSC between  
24 the parties using a real time, live stream webconference.  
25 All parties to the transaction must be registered with the  
VVSC.

27 An authentication transaction request using the VVSC

1 website necessitates that the customer use a VVSC graphic  
2 user interface (GUI) which runs from the local computer  
3 system. The GUI comprises the means for the browser of  
4 customer local computer system to display multiple images  
5 simultaneously on the monitor of said customer local  
6 computer system per the methodology of the preferred  
7 embodiment. Said multiple images further comprise: the  
8 remote parties to the transaction, the electronic data that  
9 is to be input by the parties, and the electronic document  
10 that is to be created or authenticated. Not every  
11 transaction will comprise every image, the images displayed  
are dependent on the transaction request.

12  
13 The webconference method of the inventive device will be  
14 most useful in facilitating private e-commerce transactions  
15 wherein the parties to the transaction need to ascertain  
16 the identity and actual signature of the parties to the  
17 transaction. In this aspect, geographically remote  
18 individuals may conduct high value or sensitive  
19 transactions that necessitate authentication of one's  
20 signature to the agreement using the inventive device to  
21 webconference with one another, and using the inventive  
22 device to exchange electronic data, such as an electronic  
23 signature, a photograph, a fingerprint, or an electronic  
file during the webconference.

24 Upon initiation of a webconference, the parties to the  
25 transaction may opt to upload an electronic document from  
26 the local computer system to the VVSC host computer server  
27 for electronic data input. Alternatively, the parties may  
28 elect to download an electronic document from the

1 electronic document repository maintained by the present  
2 invention. The electronic document repository comprises a  
3 library of electronic documents designed to facilitate e-  
4 commerce, including, but not limited to, deeds of trust,  
5 mortgages, promissory notes, affidavits, assignments and so  
6 on. Upon either uploading a document, or selecting a  
7 document for download, VVSC will structure the transaction  
request and manage the transaction cycle.

8

9 Per the methodology of the preferred embodiment, the  
10 electronic document to be executed is depicted along with  
11 an electronic image of the electronic signature being  
12 affixed to the document as a graphical, hand written  
13 representation or as form of source code, and the actual  
14 party executing the electronic signature. Said images are  
15 displayed on the browser of the local computer system in  
16 the manner of a screen or monitor hosted at an independent  
VVSC.

17

18 Upon affixation of each electronic signature to the  
19 electronic document, the browser of the local computer  
20 system depicts the signed electronic document. In the  
21 preferred embodiment, the electronic data may be affixed to  
22 the electronic document as a visual representation of a  
23 graphical hand-written signature. Alternatively, the  
24 electronic data may be affixed to the electronic document  
in the form of encrypted source code. Should other  
25 electronic data be required, such as a photographic image,  
26 a thumbprint, or a code, it will be entered in subsequent  
27 fashion and displayed on the browser of the local computer

1 system. By way of example, in addition to affixing an  
2 electronic signature to the electronic document, the  
3 parties may request further authentication information such  
4 as a drivers license number, a thumbprint, or a  
5 photographic image. As such other authentication data is  
6 entered, the respective information is displayed on the  
7 browser of the local computer system as a separate image,  
8 and is affixed to the electronic document where indicated.  
9 In the preferred embodiment, the electronic data may be  
10 affixed to the electronic document as a graphic, visual  
11 representation. Alternatively, the electronic data may be  
12 affixed to the electronic document in the form of  
13 encrypted source code.

14 Per the method of the preferred embodiment, the  
15 webconference is capable of providing electronic  
16 notarization services to the parties. The notary public may  
17 be an employee who is physically located at the VVSC or may  
18 be a remote party enjoined by the webconference. Electronic  
19 notarization parallels the customary legal form of  
20 notarization. The notary public shall require that the  
21 signatories provide such authentication information as  
22 required by law, typically a government issued photo  
23 identification card and a biometric submission, such as a  
24 signature or a thumbprint. VVSC employee notary public will  
25 have the means to verify hard copy personal identification,  
26 such as a drivers license information and to input said  
27 information electronically in the form of a source code.  
28 Likewise, VVSC employee notary public will have the means  
to verify the electronic signature of the party and to  
input said information electronically in the form of a

1 source code. Per the methodology above, the input  
2 information is displayed on the browser of the local  
3 computer system as a separate dual image.

4 Upon input of the personal verification information, VVSC  
5 notary public affixes an electronic notary seal to the  
6 electronic document. Per the preferred embodiment of the  
7 present invention, the electronic notary seal is in the  
8 form of a graphical representation of the notary public's  
9 seal. The graphical representation is affixed to the  
10 electronic document as a visual image. Alternatively, the  
11 notary seal may be affixed to the document in the form of a  
12 source code. Any changes to the electronic document will  
13 invalidate the notary public's seal.

14 Upon affixing the required authentication information,  
15 including, but not limited to, an electronic signature, a  
16 photographic image, biometric information, source code, an  
17 electronic notary seal, the customer uploads the electronic  
18 document to the VVSC web server from the local computer  
19 system. The VVSC fuses the respective electronic data input  
20 from the remote parties into a single, authenticated  
21 electronic document. The single authenticated document is  
22 then assigned a time and date stamp and a password. No  
23 changes may be made to the electronic document without  
24 detection. The password is disseminated to those parties  
25 authorized to retrieve a copy of the authenticated document  
26 from the VVSC web server. Logging into the server via the  
27 local computer system, authorized parties download the  
28 single, authenticated electronic document using the  
password provided from the VVSC.

1           Turning now descriptively to the drawings, in which similar  
2 reference characters denote similar elements throughout the  
3 several views, the attached figures illustrate a method of  
4 identity and signature and document authentication, the  
5 process of which is comprised of the following steps:  
6

- 7           (i)     A customer tenders a request to the process center  
8                       (hereinafter referred to as the Video Verification  
9                       Service Center) (See Figure 1-Request for Services)  
10                  for a real time, live stream video conference service  
11                  as contemplated herein. The customer's request may be  
12                  tendered in any viable medium, including but not  
13                  limited to, electronic mail; the internet; video  
14                  conference; telephone; or other means of communication  
15                  to the process unit.  
16  
17           (ii)    The Video Verification Service Center (VVSC) is an  
18                  independent location and includes affiliate locations  
19                  that offers real-time, live stream signature,  
20                  identity authentication services and document  
21                  creation and authentication services. A customer may  
22                  request a variety of verification requests,  
23                  including, but not limited to: signature verification  
24                  to execute contractual agreements, the creation of  
25                  personal identity documents such as a drivers license  
26                  or passport; notarization services; and biometric  
27                  verification requests.  
28
- 29           (iii)   The VVSC processes the customer's particular request.  
30                  VVSC will determine the services requested and the

1           parties to the transaction. (See Figure 2.) As a  
2           priori, VVSC determine:

3  
4           i. Whether the parties to the transaction have the  
5           necessary resources to utilize the invention.  
6           The distinction is illustrated in the drawings  
7           as "in-house" or "outcall". (Outcall shall  
8           presume the customer requires the necessary

9           resources to facilitate a real time, live stream  
10          conference or requires the technical skills of a  
11          VVSC representative. In-house presumes that the  
12          customer shall come to a VVSC for services);

13  
14           ii. If not, whether a representative shall bring  
15           the necessary resources to utilize the  
16           invention to the location of the respective  
17           parties, such as the home or the office; and

18           iii. If not, direct the parties to the nearest VVSC.

19  
20           (iv) VVSC will establish the time and date and locations  
21           for the real time, live stream videoconference  
22           between the customer and all pertinent parties.

23  
24           (v) The time and date will be established by a  
25           reservation system which may be manual or electronic  
26           or by other means of confirmation. All parties will  
27           receive a confirmation prior to the live stream  
28           videoconference via electronic mail or other forms of  
            messaging, such as mail or telephone.

(vi) The VVSC will implement, track and manage the services requested by the customer; irrespective of the location of the customer, throughout the real-time live stream video conference.

(vii) The VVSC can provide one or all of the following services:

- i. Electronic document creation;

- ii. Electronic document authentication through a variety of methods, including but not limited to, electronic notarization utilizing an electronic notary device, digital notarization utilizing a live notary that travels to the Client's location, an electronic signature, biometric data input or a digital certificate;

- iii. Creating and authenticating electronic signatures using biometric information or digital certificates, or other electronic data;

- iv. Electronic notarization of electronic documents;

- v. Electronic document storage and management;

- vi. Identity document or identity card creation, such as a drivers license or passport-requires and interface w/ regulatory body; or

- vii. The capture and encoding of biometric data into

1 card and document format.  
2  
3

4 (viii) The VVSC will facilitate all transactions and  
5 coordinate the involvement of outside parties and agencies  
6 if necessary. The following third party entities may be  
involved:

7 i. A traveling notary public to authenticate  
8 documents;

9  
10 ii. A traveling VVSC representative that will  
11 bring a portable, real time, live stream  
12 video conference system to the customer's  
13 location, and all necessary appendages  
14 thereto for the services contemplated  
therein; or

15  
16 iii. Government agencies or other regulatory  
17 bodies that utilize the present invention as  
18 a method to issue identity based documents  
19 or cards.

20  
21 (ix) The VVSC initiates the transaction, manages the  
22 transaction cycle and concludes the transaction. VVSC may  
23 archive the electronic document and information created  
24 therein by the use of the present invention, at the request  
of the parties to the transaction.

25  
26 (x) The present invention has unlimited applications: it  
27 serves to facilitate any transaction whereby the capture

1 and authentication of an identity, a signature, or a  
2 document is required, albeit the parties to the transaction  
3 are geographically dispersed. The invention envisions the  
4 following variations of use:

- 5 i. The present invention may be used to secure a  
6 pledge of oath.
- 7
- 8 ii. The present invention may be used to create,  
9 process and authenticate a government issued  
10 document, such as a driver's license or passport.
- 11
- 12 iii. The present invention may be used to route and  
13 facilitate the exchange of expert or professional  
14 services world-wide.
- 15
- 16 iv. The present invention may be used to create  
17 documents that require the capture of an image  
18 (i.e., one's photograph), a signature, and other  
19 personal data, including but not limited to, bio-  
metric data.
- 20
- 21 v. The present invention may be licensed to intranet  
22 environments for industry specific applications,  
23 such as banking, real estate, legal and  
24 governmental operations.

25 The present invention is an integrated system that utilizes  
26 some or all of the components as listed and described below,  
27 depending upon the transaction request. The invention operates

1       on a multi-faceted level as described below and as depicted  
2       in the following figures. To these ends, the present invention  
3       is comprised of the following components:

- 4                 (i)      a multi-point and multi-media video conference  
5                        system (including fixed and portable structures);
- 6                 (ii)     an electronic signature capture device;
- 7                 (iii)    the means to authenticate the electronic signature  
8                        input by way of the electronic signature capture  
9                        device;
- 10                (iv)     a device to create electronic documents;
- 11                (v)      the means to authenticate electronic documents;
- 12                (vi)     an electronic document repository;
- 13                (vii)    a device to create a digital certificate;
- 14                (viii)   the means to authenticate a digital certificate;
- 15                (ix)     a device to create an electronic time and date  
16                       stamp;
- 17                (x)      the means to authenticate an electronic time and  
18                       date stamp;
- 19                (xi)     a device to create an electronic notary seal  
20                       (detailed in USPTO patent-pending application,  
21                       identified as Customer 021907);
- 22                (xii)    the means to authenticate an electronic notary seal  
23                       (detailed in USPTO patent-pending application,  
24                       identified as Customer 021907);

- (xiii) a device or devices to capture biometric data, such as a fingerprint, photographic image and the like;
- (xiv) the means to authenticate biometric data, such as a fingerprint, photographic image and the like;
- (xv) a device to fuse the electronic data input with an electronic document;
- (xvi) the means to authenticate an electronic document that has electronic data fused to it; and
- (xvii) such other applications and or devices which are necessary to facilitate the function of the aforementioned components whether individually or in conjunction with one another.

## OPERATION OF THE INVENTIVE DEVICE

## 1. MULTI-POINT, MULTI-MEDIA VIDEO CONFERENCE SYSTEM

As a priori, a video-conference or video communicating system will be necessary for the method of the present invention. The video-conference system of the present invention will utilize, including but not limited to, a multi-point, multi-media video-conference or video-communication system, a video-conference server, and a video-conference administration server that will simultaneously deliver video and voice information along with various types of electronic and material data necessary to verify personal identity, signatures and

1 documents. The method of the present invention will be  
2 capable of delivering media in various formats, including  
3 but not limited to, video clips, audio, text, and graphics.

4  
5 The video-conference system of the present invention will  
6 utilize the various structures and technology of the prior  
7 art as referenced above, and other existing video  
8 conference systems, including but not limited to, hand-held  
9 devices, portable devices, telephonic devices, cellular  
devices, and satellite devices.

10  
11 **2. ELECTRONIC SIGNATURE CAPTURE DEVICE**

12 An electronic signature capture device will be necessary  
13 for the method of the present invention. The function of  
14 the electronic signature capture device will be to capture  
15 the electronic signatures of the parties to the transaction  
16 and transmit this data as necessary. The electronic  
17 signature capture device will be capable of assigning  
18 digital code and or graphic images as a means of signature  
19 authentication. The graphical representation depicts the  
actual hand-written signature of the signatory.  
20 Additionally, the electronic capture device may be used to  
21 input an electronic notary seal.

22  
23 **3. DIGITAL CERTIFICATE**

24 A digital certificate will be necessary for the method of  
the present invention. The function of the digital  
25 certificate will be to authenticate either identity or  
26 documents. Additionally, the VVSC may issue a digital  
27 certificate as a form of personal identity verification  
upon registration with the VVSC for webconference services.

1           **4. ELECTRONIC NOTARY DEVICE**

2       An electronic notary device will be necessary for the  
3       method of the present invention. The function of the  
4       electronic notary device will be to provide electronic  
5       notarization to electronic documents. The electronic notary  
6       stamp is affixed to the electronic document in one of two  
7       ways: by manually imprinting the notary seal using the  
8       electronic signature capture device pad and the  
9       conventional notary stamp, or, alternatively, by utilizing  
10      an electronic device that is encrypted with the equivalent  
11      of the notary's stamp in the form of source code which is  
12      affixed to the electronic document. The present invention  
13      will electronically affix the electronic notary seal to  
14      verify either a signature that is in a graphical format  
15      (using an electronic signature capture device) or an  
16      electronic format (using a digital certificate).

17           **5. BIOMETRIC DATA CAPTURE DEVICE**

18       A system to capture and process bio-metric data, including  
19       but not limited to, a signature, a fingerprint, a  
20       handprint, a voice print, a photograph, and retina  
21       information, will be necessary for the method of the  
22       present invention. The function of the biometric input  
23       system will be to affix personal characteristics as  
24       identified herein in the form of source code to an  
25       electronic document or identification card as a means of  
26       authentication.

27           **6. ENCRYPTION CODE**

28       An encryption system will be necessary for the method of  
the present invention. The function of the encryption

1 system will be to authenticate and secure the electronic  
2 document or identification card that is created by the  
3 present invention.

4

5 **7. ELECTRONIC DOCUMENT REPOSITORY**

6 An electronic document repository will be necessary for the  
7 method of the present invention. The function of the  
8 electronic document repository will be to create, transmit,  
9 manage and store electronic documents that are created or  
authenticated by the present invention.

10

11 **8. HOST COMPUTER SYSTEM**

12 A processing center comprised of a main, regional and local  
13 servers will be necessary for the method of the present  
14 invention. The processing center will track incoming and  
15 outgoing electronic messages; track customer accounts and  
16 identities; archive all relevant information for future use  
17 and/or reference; and disseminate the foregoing data to  
18 regional/local servers and clients as necessary. The main  
19 server shall structurally serve to store all of the  
20 information generated by the invention and its related  
21 processes, systems, and methods. The interconnections  
22 between the servers include any and all networks and/or  
23 systems or applications that facilitate the use of the  
24 present invention, and any and all infrastructure necessary  
25 to facilitate authentication utilizing the present  
26 invention. The processing centers will serve as physical  
27 structures that facilitate requests or route them to  
independent affiliates with the resources to conclude the  
transaction requested.

All of the components of the present invention serve to work as an integrated whole; however, they are not necessarily utilized all at once. The relationship of the components is dependent on the transaction contemplated. Nonetheless, all of the invention's components will serve to interface with the real time, live stream videoconference transaction. That is, the processes and functions of each component will be integrated into the videoconference process for a relatively simultaneous transaction. Said interface will be in the form of permanent and portable devices that are compatible with the videoconference system being utilized. The invention will also employ any software and hardware applications as necessary to make the invention function as an integrated whole.

The prior art fails to provide an integrated method of simultaneously accomplishing multiple tasks as depicted above. The present invention is able to enjoin and authenticate several transactions in a single process. It is also applicable to any transaction where one's identity, signature or a document requires authentication.

#### **DEFINITIONS**

Given the possible breadth of the present invention's potential, it is to be understood that the following terms as used anywhere in the application herein shall be construed to have the following meanings:

1                   **Transaction:** The term "transaction" should be given a  
2 broad reading because it encompasses a vast array of  
3 possible applications of the present invention. For  
4 example, the present invention can authenticate  
5 electronic documents that require a notary public to  
6 authenticate the signature and the corresponding  
7 electronic document; e-commerce documents that require  
8 that the identity of a party be verified; signature  
9 verification, document authentication; documents that  
10 must be signed by the parties simultaneously to take  
11 effect, or identification cards and documents that  
12 require identity authentication. Likewise, the present  
13 invention may be utilized in industry specific  
14 environments, such as banking, real estate, legal and  
15 governmental operations.

16                   **Videoconference:** The term "videoconference" or  
17 "webconference" and the various verb permeations  
18 thereof shall be construed to mean a process that is  
19 being conducted real time using live stream data and  
20 technology. The present invention may use various  
21 videoconference technology and applications thereof,  
22 but all are premised on the fact that it is a real  
23 time, live stream transaction.

24                   **Notary public:** The term "notary public" or  
25 "notarization" shall be construed to mean  
26 authenticating a document using, but not limited to,  
27 the following means: a live commissioned notary  
28 public; another person certified to authenticate

1 documents; digital forms of notarizing documents such  
2 as a digital certificate and the technology identified  
3 in United States pending patent application, herein  
4 identified as Customer 021907.

5 **Electronic Document:** The term "electronic document"  
6 shall be construed to mean any data that is  
7 constructed and compiled by use of the present  
8 invention; including but not limited to, digital or  
9 electronic documents in various mediums, whether  
10 tangible or not (i.e. source code, compact disc,  
11 floppy diskette, etc.); documents encompassing an  
12 array of transactions and documents comprised of  
13 tracking, managing and storing information created by  
use of the invention.

14 **Electronic Signature:** The term "electronic signature"  
15 shall be construed to mean any form of electronic  
16 signature, including but not limited to, a graphical,  
17 hand written representation using a signature capture  
18 device, a digital certificate, a password, or such  
19 other electronic data input.

20 **Biometric Data:** The term "biometric data" shall be  
21 construed to mean any form of biometric information  
22 including but not limited to: a fingerprint, a  
23 handprint, a voice print, a retina print, an  
24 electronic signature, a manual signature, sources of  
25 DNA reducible to electronic code and personal  
26 information in the form of electronic input: such as  
27 height, weight, color, shape and size.  
28

1                   **Electronic Data:** The term "electronic data" shall be  
2                   construed to mean any form of electronic data input,  
3                   including but not limited to: an electronic signature,  
4                   biometric data, source code, passwords, graphics,  
5                   audio and other such electronic data.

6  
7                   As to a further discussion of the manner of usage and  
8                   operation of the present invention, the same should be  
9                   apparent from the above description. Accordingly, no  
10                  further discussion relating to the manner of usage and  
11                  operation will be provided.

12  
13                  With respect to the above description then, it is to be  
14                  realized that the optimum dimensional relationships for the  
15                  parts of the invention, to include variations in size,  
16                  materials, shape, form, function and manner of operation,  
17                  assembly and use, are deemed readily apparent and obvious  
18                  to one skilled in the art, and all equivalent relationships  
19                  to those illustrated in the drawings and described in the  
20                  specification are intended to be encompassed by the present  
invention.

21  
22                  Therefore, the foregoing is considered as illustrative only  
23                  of the principles of the invention. Further, since  
24                  numerous modifications and changes will readily occur to  
those skilled in the art, it is not desired to limit the  
25                  invention to the exact construction and operation shown and  
described, and accordingly, all suitable modifications and  
26                  equivalents may be resorted to, falling within the scope of  
27                  the invention.